Distributed Security Architectures

First Quarter 2003 Progress Report

Covers work done Oct through Dec, 2002.

Personnel:

Staff: Mary Thompson, Abdelilah Essiari, Keith Beattie

Student: Jeiwei Lin

Akenti interfaces

Added a C/C++ compatible interface to both the policy engine and the Akenti Client to return conditional as well as unconditional actions. This interface returns an capability class or structure and provides methods to extract the unconditional actions, to extract to conditional actions and to iterate over the conditions, evaluating them and returning the currently allowed actions. The caller must provide an evaluator function that evaluates a single term of the condition. Our library does the parsing of the expression and the combining of the terms. The next version of the Globus Job-Manager will use this implementation which will greatly simplify it.

Akenti Policy Engine

The Akenti server's use at PPPL as part of the Fusion Collaboratory revealed a few bugs that were fixed. The LDAP search code needed to be updated to handle referrals from the DOE Grids CA. Our handling of DN's needed to be made a bit more general in order to correctly handle the DOE Grids host certificate names which contain '/'s.

More progress was made on compiling the code with the g++3 compiler and the Sun compiler was added as well. Each C++ compiler has trouble with different code constructions. Our intent is to get the Akenti code to work compile with a range of current C++ compilers.

Certificate Generators

The certificate generators can now either be run independently, or use a server or file for hints to preload fields of the GUI interface. The comments and help dialogues were also improved and updated to reflect the changes. A reader class was added to support PKCS8 files, so that a user can sign the certificates with his private key in either a pkcs8 or pkcs12 format file.

The generators can now talk to a Resource Definition server either through HTTP or HTTPS. The motivation for this change is to allow newly created certificates to be uploaded securely to the resource server machine.

Code Distribution

We released an updated version of the code at the end of December. It includes the newest C interfaces to the Akenti server, a C++ version of the command line program that creates certificates to replace the Java one and better examples and documentation on how to use the release.

Collaboration with Other Projects

Implementation of the C++ security shared library continued. This library will facilitate sharing of high quality implementations of commonly used security functions among the Secure and Reliable Group Communication project, the Peer to Peer File Sharing project and Akenti.

The Akenti policy engine was wrapped in a Python Grid Services interface for a SC02 demo. This was a joint effort of the Distributed Security Architecture project and the Grid Services project. It demonstrated the use of the Grid Services wrapping tools to take an existing service and rapidly turn it into a Grid Service.